Amendments to the Claims

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of claims:

1. (previously presented) A method of digitally signing a plaintext message exchanged between a pair of correspondents in a data transmission system, one of said pair of correspondents being the signer and having a private key *a* and a public key derived from the private key *a*, said public key being available to the other of said pair of correspondents, said method comprising the steps of:

subdividing said plaintext message into a first plaintext bit string H and a second plaintext bit string V;

computing a first signature component *c* as a function of said first plaintext bit string H wherein the plaintext bit string H is hidden in said signature component *c*;

computing an intermediate signature component *c'* as a function of said first signature component *c* and said second plaintext bit string V;

computing a second signature component *s* as a function of said intermediate signature component *c'* and said private key *a*; and

forming a signature (s,c,V) containing said first signature component *c*, said second signature component *s*, and said second plaintext bit string V as discrete signature components;

whereby during verification, said second plaintext bit string V is available from said signature (s,c,V) as an input to a verification protocol.

2. (previously presented) A method according to claim 1 wherein redundancy in said first plaintext bit string H is compared to a predetermined level prior to computing said first signature component *c*.

3. (previously presented) A method according to claim 2 wherein said redundancy is adjusted to exceed a predetermined level.

4. (previously presented) A method according to claim 3 wherein data is added to said first plaintext bit string H to adjust said redundancy.

5. (previously presented) A method according to claim 4 wherein an indicator is included in said first plaintext bit string H to indicate additional data.

6. (previously presented) A method according to claim 1 wherein said second signature component *s* is generated by hashing said first signature component *c* and said second plaintext bit string V.

7. (previously presented) A method of verifying a plaintext message from a signature of a purported signer in a data transmission system, said plaintext message being subdivided into a first plaintext bit string H and a second plaintext bit string V, said signature formed as a set of discrete components, said signature containing a first component computed as a function of said first plaintext bit string H whereby said bit string H is encrypted therein, and said second plaintext bit string V as a second component, said purported signer having a private key used in the computation of said signature and a corresponding public key available for use in verification, said method comprising the steps of:

generating a value by combining said first component with said second plaintext bit string V;

recovering said first plaintext bit string H from said value using publicly available information of the purported signer including said public key;

examining said recovered first plaintext bit string H for a predetermined characteristic; and

verifying said message if said predetermined characteristic is present.

8. (previously presented) A method according to claim 7 wherein said combination of said first component and said second plaintext bit string V includes hashing a combination of said first component and said second plaintext bit string V.

9. (previously presented) A method according to claim 7 wherein said predetermined

characteristic is the redundancy of said recovered first plaintext bit string H.

10. (previously presented) A method according to claim 9 wherein said signature includes a third component derived from a combination of said first component and said second plaintext bit string V and said first plaintext bit string H is recovered utilising said third component.

11. (previously presented) A method according to claim 1 wherein said first signature component *c* is computed by applying a function to said first plaintext bit string H and said first plaintext bit string H may be recovered from said first signature component *c* by applying a complementary function to said first signature component *c*.

12. (previously presented) A method according to claim 11 wherein said function is encryption with an encryption key, a decryption key is computable from information available in said signature, and said complementary function is decryption with said decryption key.

13. (previously presented) A method according to claim 12, wherein said encryption key is a short-term derived from a random integer used in the provision of said second signature component.

14. (new) A method, for authenticating a communication between a first correspondent and a second correspondent in a data transmission system, said first correspondent having a private key *a* and a public key derived from the private key *a*, said public key being available to said second correspondent, said method comprising:

said first correspondent subdividing a plaintext message into a first plaintext bit string H and a second plaintext bit string V;

said first correspondent computing a first signature component *c* as a function of said first plaintext bit string H wherein the plaintext bit string H is hidden in said signature component *c*;

said first correspondent computing an intermediate signature component *c'* as a function of said first signature component *c* and said second plaintext bit string V;

said first correspondent computing a second signature component *s* as a function of said intermediate signature component *c'* and said private key *a*;

said first correspondent forming a signature (s,c,V) containing said first signature component *c*, said second signature component *s*, and said second plaintext bit string V as discrete signature components;

said first correspondent making available to said second correspondent, at least said first signature component *c* and said second plaintext bit string V;

said second correspondent generating a value by combining said first signature component *c* with said second plaintext bit string V;

said second correspondent recovering said first plaintext bit string H from said value using publicly available information of said first correspondent including said public key;

said second correspondent examining said recovered first plaintext bit string H for a predetermined characteristic; and

said second correspondent verifying said message if said predetermined characteristic is present.